

Certification

This is to certify that the foregoing translation of the document entitled "Method And System For Verifying An Electronic Instrument For Metrological Measurements" was made from Italian to English by me. I am a competent translator well acquainted with both languages, and that, to the best of my knowledge and belief, it is a true and complete rendering into English of the original document.

Date: 9-9-2008


Robert Endoy

Summary of the invention, with main drawing, description and claims

Application number: M12002A 002419 Filing date: 11-15-2002

Patent number: Date issued:

Title

“Method and system for verifying an electronic instrument for metrological measurements ”

Summary

Verification system for an electronic instrument for metrological measurements, comprising a local electronic processing unit including a control application of said instrument. The system comprises a verification application for said control application, which can be associated to said local processing unit, and said verification application being suitable for generating a univocal certification code for the application.

DESCRIPTION of the industrial invention

In name of: NUOVO PIGNONE HOLDING S.P.A.

Nationality: Italian

Place of business in: Florence

The present invention relates to a method and system for verifying an electronic instrument for metrological measurements.

In particular, the present invention relates to a method and system for verifying an electronic instrument for metrological measurements comprising a control application for the measurement performed by the instrument.

Such metrological measuring instrument can be, for instance, an instrument installed inside a fuel distributor, suitable for measuring the quantity of supplied fuel.

For the purpose of the present invention, by control application for metrological measurement is understood a software tool or a processing program which acquires, processes, displays and prints the data inherent to the performed measurement.

It is known that metric instruments are subjected by law to periodic inspections, which consist in verifying over time their metrological reliability, and are aimed at protecting the integrity of seals, also electronic, and labels or other protection elements foreseen by the existing standards.

An authorized operator (Metrology Auditor) is tasked with performing such inspections, which relate, for instance, to the structural integrity of the measuring instrument, as well as to the integrity of the applications or processing programs contained in said instrument.

By integrity of the applications is understood that the applications did not undergo interventions capable of modifying the integrity and originality of the software application that controls the metrological measuring instrument.

At the present time, said seals that guarantee the integrity and originality of the application are hardware type seals, for instance lead seals.

The applicant has observed that these inspections require said assigned operator (Metrology Auditor) to go to the place where the measuring instrument is located and to verify the integrity of these hardware seals. In case the supplier of the application releases a new updated version of this application, the metrology auditor must go to the location to remove said seals and install others, after the correct function of the updated version of the application has been verified.

The Applicant has taken on the problem of simplifying the certification operations of software applications for simple electronic instruments for metrological measurements and making them reliable.

The Applicant has created a method and a system for verifying an electronic instrument for metrological measurements in which a verification application, residing in an electronic processor connected with said measuring instrument, for instance through a network, verifies whether the application controlling the measurement performed by the instrument was altered, tampered with, modified or other. A stamp of authenticity is issued based on the outcome of the verification of the control application of the instrument.

Preferably, the verification application determines whether the control applications satisfy the following conditions:

- the control application installed on the instrument must conform to what was certified at the start-up of the instrument.
- the control application installed on the instrument must not be unduly tamperable.
- any deviation in the control application installed on the instrument must be evident and identifiable.
- the presence of a different control application must be identifiable,
- the employed techniques must ensure that all above mentioned actions are performed in a context of data security, using the appropriate encryption techniques, digital signature controls, certificates, etc.
- all relevant actions within the scope of changes of the executable programs of the instrument must be recorded on supports that cannot be modified by third parties.

In general, the controls are suitable for allowing an indisputable reconstruction of the actions performed on the control application of the instrument:

One aspect of the present invention concerns a verification system for an electronic instrument for metrological measurements, comprising one local electronic processing unit including a control application for said instrument, characterized by the fact of comprising a verification application for said control application, which can be associated to said local processing unit, said verification application being suitable for generating a univocal code for certification of the application.

Another aspect of the present invention concerns a method for verifying an electronic instrument for metrological measurements, said instrument being associated to a local electronic processing unit including a control application of said instrument, comprising the following phases:

- receiving, when the control application is started, information regarding the control application contained in said local unit,
- processing this information through a comparison with pre-memorized information,
- issuing a univocal certification code that can be associated to said control application,
- printing a stamp containing said univocal code on paper support.

The characteristics and the advantages of the method and of the system for verifying metrological measuring instruments according to the present invention will become more clear and evident from the following description, given as a non-limiting example, of an execution form with reference the attached figures in which:

Figure 1 is a block diagram of the verification system according to the present invention applied to generic “client” applications;

Figure 2 is a block diagram of the verification system according to the present invention applied to a fuel filling station for vehicles;

Figure 3 is a representation of a “software stamp” according to the present invention;

Figures 4a-e show viewing screens of the verification application according to the present invention.

With reference to the cited figures, the system according to the present invention comprises by preference a central processing unit 2 (server) and at least one local processing unit 3, which contains at least one control application 4 for a metric instrument. By preference, said central processing unit comprises also a control application 4 for a metric instrument.

The connection between the central unit and the local units is by preference obtained through a traditional communication network, for instance an LAN network, an Ethernet network or through Internet connection. In general, said network allows the use in said local units of applications or programs, physically resident in a memory of said central processing unit.

In figure 1, three local stations are shown as an example, since the system of the present invention is also capable of controlling at the same time a plurality of local units. One of the

local units illustrated in figure 1, comprises two control applications 4 for an electronic instrument for metrological measurements, since the system of the present invention controls at the same time in equivalent manner one or a plurality of applications installed inside the same local unit.

Said central processing unit comprises by preference at least one verification application 21 of said control applications, in addition to at least one central application 22.

By preference, both the central processing unit and the local units contain at least one dynamic library 6 of functions that can be associated to said verification application 21, which acts as a link between the control applications and the verification application.

Figure 2 illustrates an application example of the verification system according to the present invention applied to a fuel filling station for vehicles, indicated as a whole by the numerical reference 7.

The filling station comprises, at least one fuel distributor 71, which contains internally said metrological measuring instrument suitable for measuring the quantity of fuel supplied by a fuel pump. One local processing unit associated to said distributor comprises said control application, as previously described, which controls the measuring instrument.

In addition, said station comprises an automatic distribution column 72, suitable for activating the distributors in absence of personnel attending to the distribution. Such column is activated following the insertion in it of an appropriate quantity of money, through bank notes or credit cards, Bancomat and similar. Inside such column is present, for instance, another local processing unit.

Additional local processing units are installed, for instance, in distribution and/or sales points of service station products 74, in accounting and/or administrative offices 75.

According to the example of figure 2, the central processing unit 73 connects the cited local processing units so as to form a network.

According to the present invention, the verification application is preferably contained in the central unit 73. Alternatively, in case the filling station is not provided with a network but comprises at least one local processor associated to a metrological measuring instrument, said verification application is installed inside said local unit.

The control application of the measuring instrument is preferably provided with a certification of authenticity, which is supplied by the author of the application. Such certification comprises a digital signature implemented, for instance, through a RSA cryptography protocol.

Through a mechanism of public and private keys, such digital signature guarantees the authenticity of the control application to which such key is associated.

A known technology that implements such digital signatures is the Microsoft® Authenticode™ technology that verifies that a given application disposes of a valid certificate, or that the identity of the producer of the application corresponds to what is certified and that the certificate is still valid. This is obtained by attaching a digital signature to the software code that allows remote users to verify the trustworthiness of the editor of the application.

According to the present invention, the verification application is capable of reading such digital signatures and of recognizing their authenticity. In case the authenticity is not verified, the verification application issues a message and interrupts the start-up of the control application containing the invalid digital signature.

Furthermore, the verification application acquires some information about the unit in which the application to be verified resides, in order to create a unique information context linked to the unit itself. Examples of possible information that can be useful for verifying the application are:

- serial number of the network board,
- serial number of hard disk,
- univocal identification of the processor, etc.

In case of network configurations, the verification application identifies in univocal manner also the machines present in the network through its own local component for the application, in order to be able to react to any variations of the network configuration.

Once all of the previously described information has been acquired, the verification application processes all the data and creates a synthesis of limited dimension. For instance, the synthesis can be obtained through so called "hashing" (SHA, RSA, etc.) cryptographic algorithms and generates a univocal code which is defined as "software stamp", which is printed by said local unit and associated to the verified control application.

By preference, this univocal code can be printed, for instance, in the form illustrated in figure 3, which refers to the certification of a control application named SINP version 2.0.1 produced by the Applicant and released on 09.13.2001. In addition, such stamp 8 displays a print date 81 of the stamp, a code 82 of the filling station, a barcode 83 corresponding to said univocal code of the software stamp.

The control application works in the following manner. At the start-up of the control application 4 to be verified, the verification application 21 is called up automatically through said dynamic library 6 associated to the control application in the local unit.

The information about the control application is acquired through this library. The application is validated by using the verification of said application certificate, for instance, according to the rules of the Microsoft® Authenticode™ standard.

The verification application 21 acquires some information about the local processing unit 3 on which resides the control application 4, in order to create a unique context of information for the identifiability of the unit itself. In case of network configurations, the control application identifies in univocal manner also the other units present in the network through every dynamic library 6 present in each local unit, in order to be able to react to any variation in the configuration of the network itself.

Once all the information mentioned in the preceding points has been acquired, a 'software stamp' is issued as described previously, which is memorized in said local processing units and linked to the verified control application.

By preference, all operations performed by the verification application on the control application to be verified, are memorized in a file, of which the integrity and consistency are controlled to verify that no manipulations or cancellations have occurred. Any incongruities found in this phase generate a message and prevent the launch of the applications.

In case one wishes to update the control application, for instance, by installing a new version, the verification application determines the emission of a new software stamp.

In particular, the verification application determines that the application has changed, and is no longer consistent with the pre-memorized information, through the software stamp. In this case, the authenticity of the new version of the control application is verified.

This verification is performed mainly in three steps:

- It is verified that the new version was made by the same producer of the preceding version, through said digital signature;
- It is verified that the new version is successive to the preceding (for instance version 1.2 instead of version 1.1)
- It is verified that this version is consistent with other applications with which the local processing unit cooperates.

Once these steps executed, the verification application will propose to the user the creation of a new software stamp. The software stamp represents the necessary evidence at the

nonnative level for properly controlling the release of new versions. Concretely, all this is obtained through printing on paper support and producing a model as shown in the example in figure 3.

Figures 4a-e represent some examples of input and/or display masks generated by the verification application during the survey of a control application.

Figure 4a illustrates a first mask 91, which at the start of the control application of the measuring instrument, shows the univocal code of the software stamp. In this case there was no modification in the verified control application and by pushing on the "ok" key the control application is launched correctly. This mask is optional, in the sense that this mask can be displayed in cases of control applications requiring the presence of a user at start-up. In cases where the application starts-up automatically, for instance, concurrently with the powering up of an installation, this mask is omitted.

Figure 4b illustrates a second mask 92, which displays a change that took place in the configuration of the local processing unit. Such change can be, for instance, an update of the control application version or a change in the hardware and/or software configuration of the processing unit. In this case, a comparison mask 93 is displayed, in which such changes are listed. In particular, the upper box 931 of this mask shows the new applications and/or new versions of the application present in the local unit and the lower box 932 shows the substituted parts. The new configuration shown in said upper box, needs to be confirmed through a push button in the lower part of the screen; the confirmation operation is equivalent to declaring that the changes are conform to the above mentioned authentication conditions. Following this confirmation, a new univocal code is issued and a new software stamp is printed.

At this point, the univocal code can be entered in said second mask 92 and following the confirmation, by pressing the "ok" key, the system proposes a third mask 94 in which is requested to confirm (yes/no) that the performed modifications are conform to the metric verification standards of the measuring instrument.

In case of confirmation (yes), the system proposes a fourth mask 95 which communicates that the operations were performed correctly and allows proper start up of the control application. In case of no confirmation (no), the system proposes a fifth mask 96, which communicates the inability to start up the application correctly, because the metrological operations were not completed. In this case the application can only be launched to perform functional tests.

In order to ensure the natural evolution followed by the verification application during its life cycle, the application is by preference developed according to criteria of modularity, reusability of the code and transferability. Compliance with these requirements guarantees that new functions can be added with limited impact. For this purpose, where applicable, it is preferred to use programming languages of the type known as "object oriented".

Furthermore, it is preferred to use techniques that make applications and data formats as much as possible independent from each other. In this way, the application is prepared for possible data format changes and is advantageously compatible with other applications, devices or systems.

To ensure the maintainability of the verification application code, any public interface, public data and function is documented. The system variables have by preference mnemonic names and comply with the writing notations of the code typical for the development environment (prefixes indicating the type of data, etc.). Every public function or method is appropriately documented through a description in the function itself and for each parameter is specified by a functional description comprising the validity interval and the use in input or in output of the parameter itself.

By preference, the error codes are consistent with the other parts of the application and are available from a univocal source (index or resource file). In any case, every error code generated by the application is documented and memorized in the events file of the application.

Compliance with the requirement of longevity of the application implies inevitably the choice of architectures which are likely to be supported for a time period equal or superior to the estimated life of the application itself.

The verification application, in accordance with the present invention follows closely the operational modes, the terminologies and the documents already known to the users of the control application and of the metrological measuring instrument, so that the user himself perceives the procedure as "familiar". In any case, interfaces and masks are as much as possible clear and simple. Advantageously, the most frequent operations are performed with the least possible number of passages.

All the operations of the verification application are coherently grouped in functional areas, to make them easily available. The functions are accessed preferably through pushbuttons or, where applicable, through menus, hypertexts or icons. Parts indicating data or commands must be large enough to be clearly legible. However, the dimensions of the interface objects must not be excessive, in order not to render the objects dispersive.

Ing. Barzano & Zanardo Milano S.P.A.

Claims

1. Verification system for an electronic instrument for metrological measurements, comprising a local electronic processing unit including a control application of said instrument, characterized by the fact of comprising
 - a verification application for said control application, that can be associated to said local processing unit,
 - said verification application being suitable for generating a univocal code for metrological certification of the application.
2. Verification system according to claim 1, in which said univocal code is associated to printing of a stamp comprising the issue date of said stamp (82), a reference code of the metrological measuring instrument, a barcode (83) corresponding to said univocal code.
3. Verification system according to claim 1, in which said verification application is associated to a central processing unit, which is connected with said local unit through a telecommunication network.
4. Verification system according to claim 1, characterized by the fact of comprising a dynamic library, associated to said control application which, at the start of the control application, calls up said verification application.
5. Verification system according to claim 4, in which the dynamic library is located in said local unit.
6. Verification system according to claim 4, in which said dynamic library is located in said central processing unit.
7. Verification system according to claim 1, in which said univocal code is obtained through a cryptographic algorithm.
8. Method for verifying an electronic instrument for metrological measurements, said instrument being associated to a local electronic processing unit including a control application for the instrument, comprising the following phases:
 - receiving, at the start of the control application, information contained in said local unit concerning the control application,
 - processing this information through a comparison with pre-memorized information,
 - issuing a univocal certification code that can be associated to said control application,

- printing a stamp containing said univocal code on paper media.
9. Method according to claim 8, in which said phase of issuing a univocal code comprises processing said information according to a cryptographic algorithm.
 10. Method according to claim 8, in which said phase of receiving information comprises the phase of receiving a certificate of authenticity of the control application.
 11. Method according to claim 8, in which said phase of receiving information comprises the phase of receiving an identification code of said local unit.

Ing. Barzano & Zanardo Milano S.P.A.

[Fig 1]

Software controllo autenticità: authenticity verification software

Fig. 3

Applicazione: application

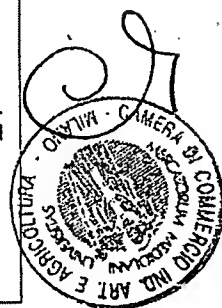
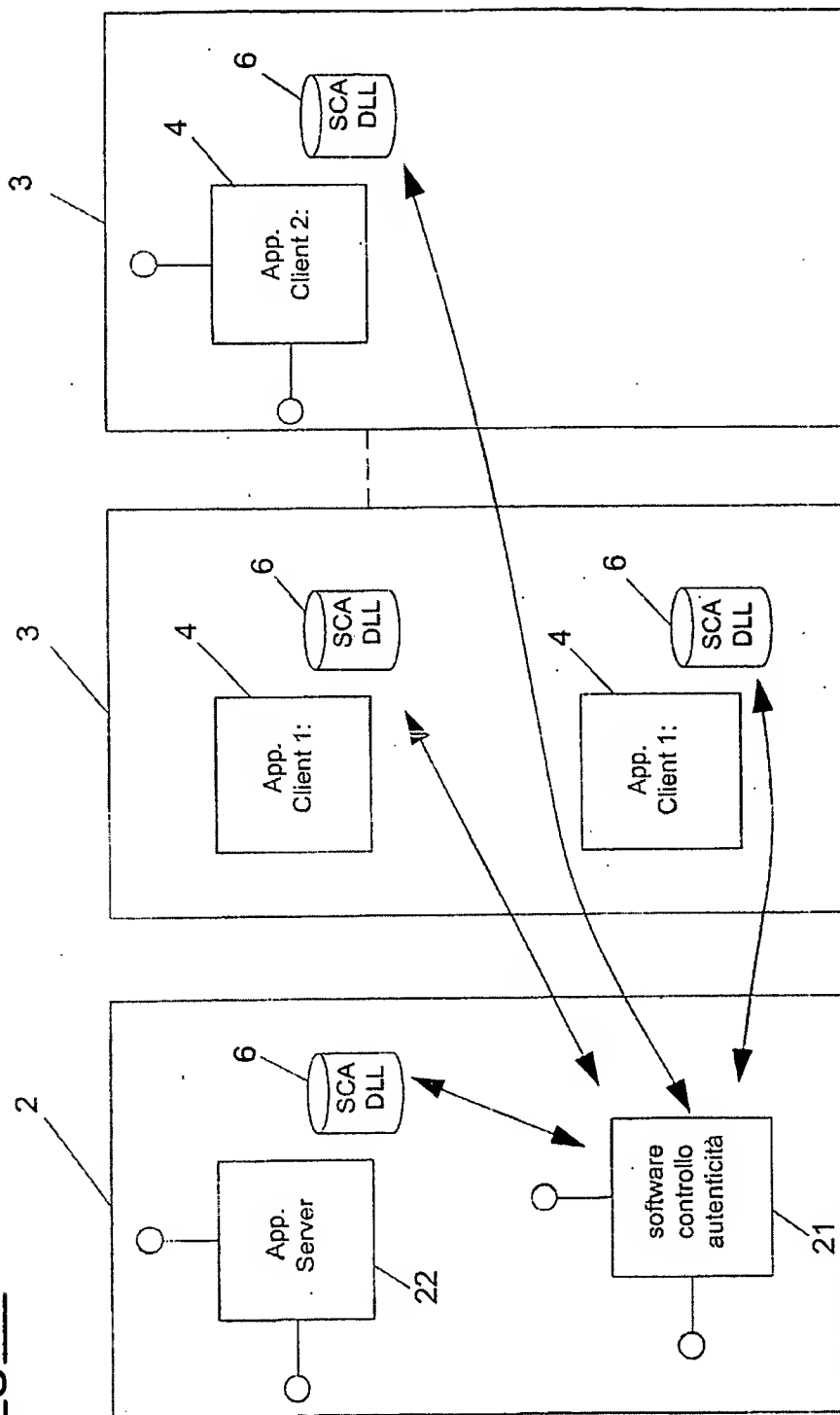
Versione: version

Data: date

Staz. di servizio: filling station

Stampato il: printed on

Fig. 1



I MANDATARI
(firma)

R. E. T. Lias
(per sé e per gli altri)

MI 2002A 0 02415

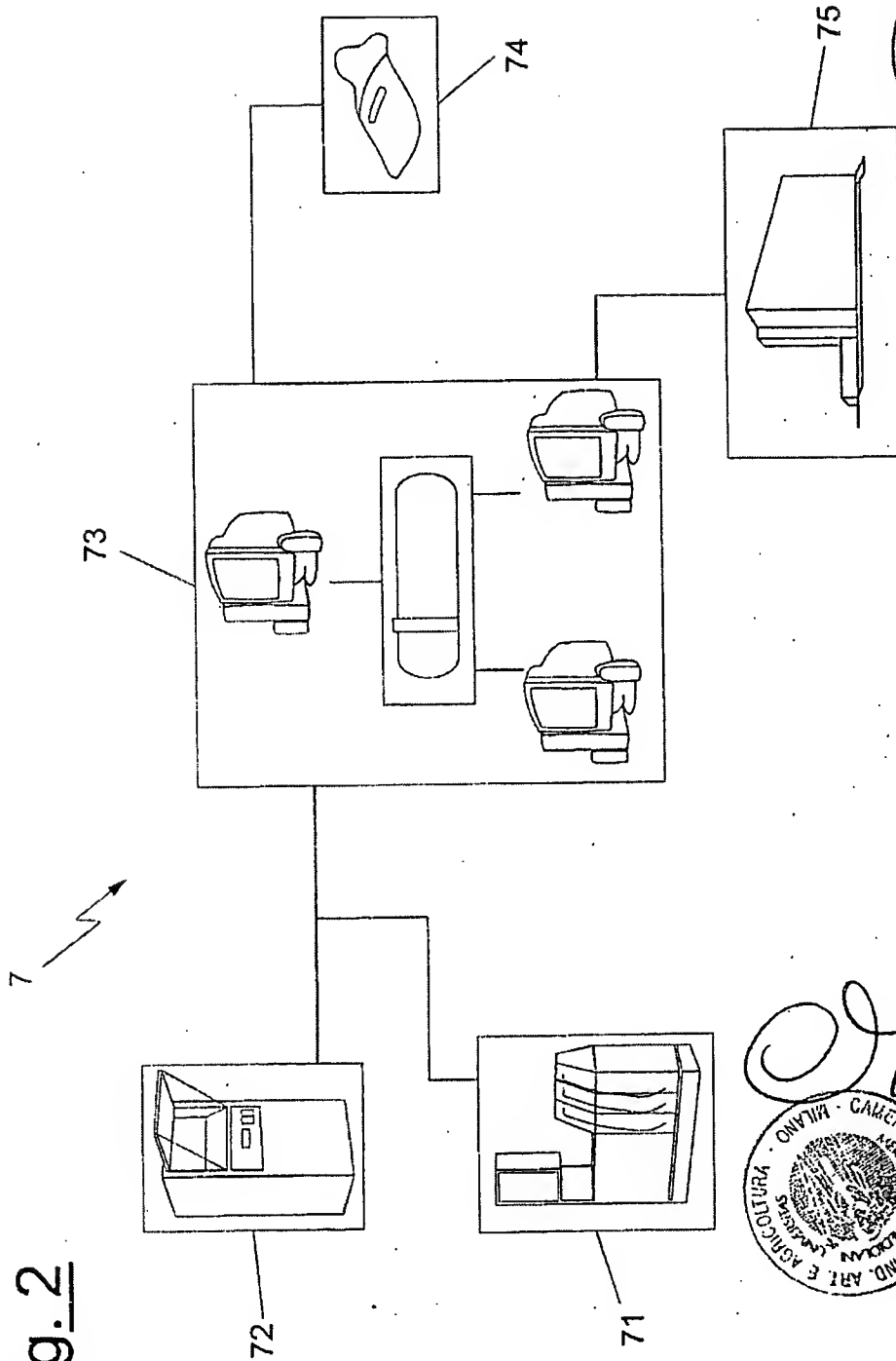


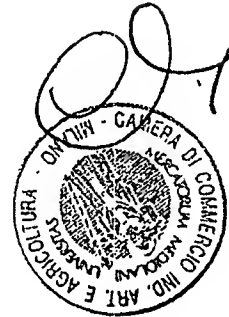
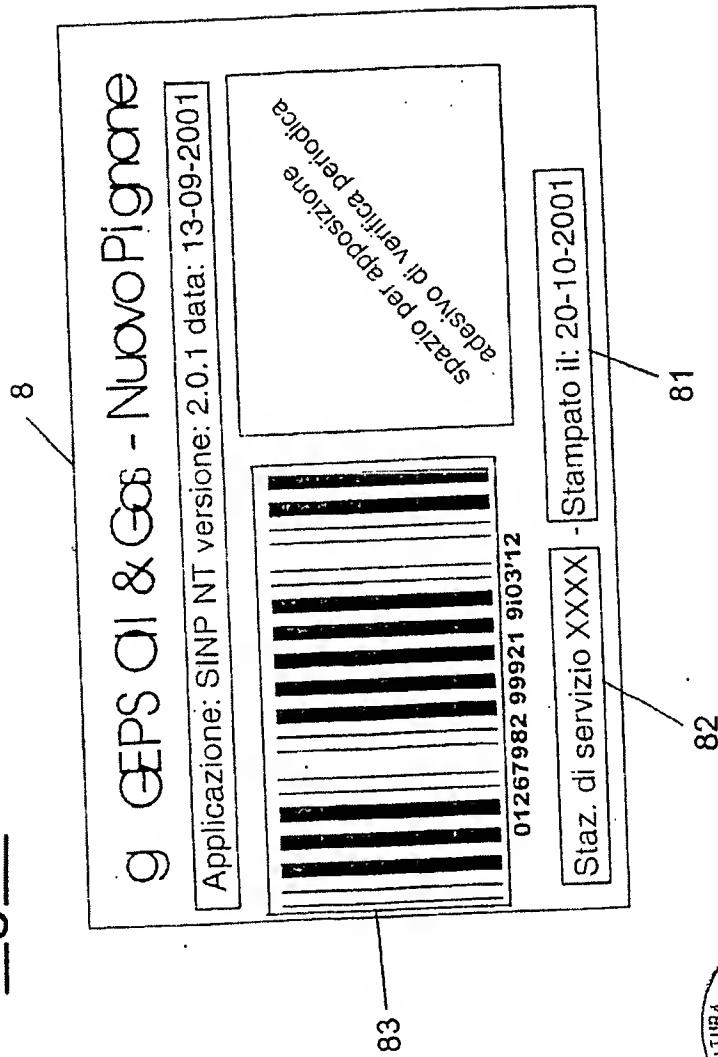
Fig. 2

I MANOVA
(firma)

R. E. T. Dias

MI 2002A 002419

Fig. 3



E. T. Khan

Fig. 4a

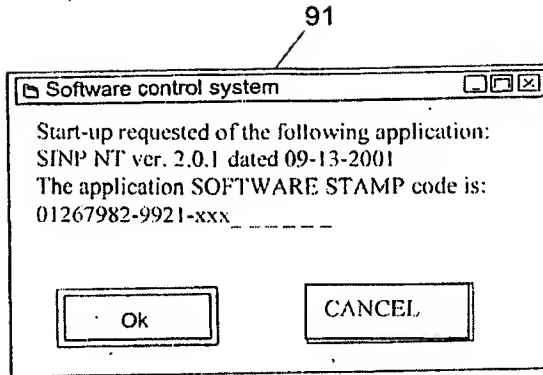


Fig. 4b

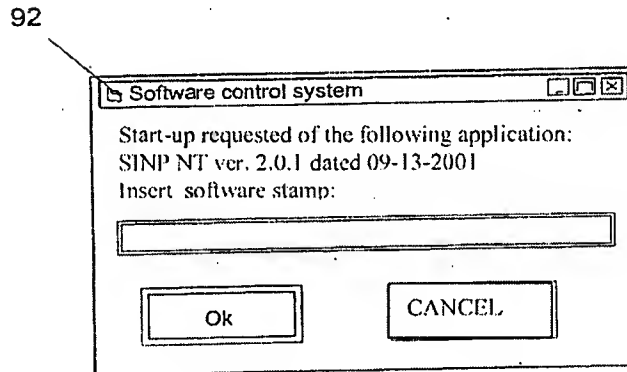
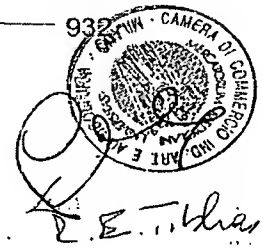
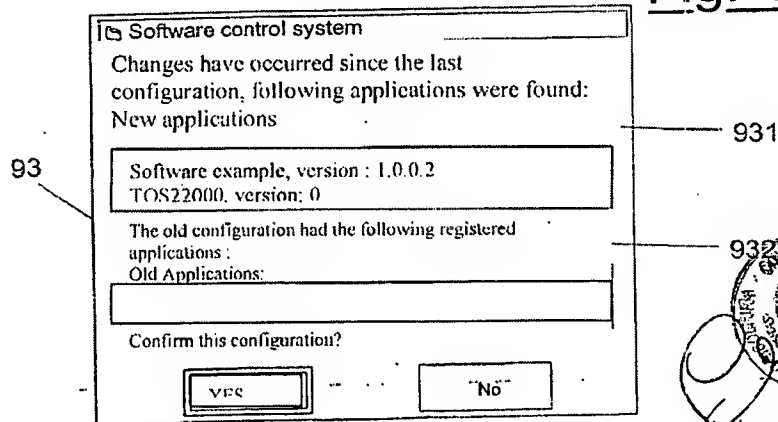
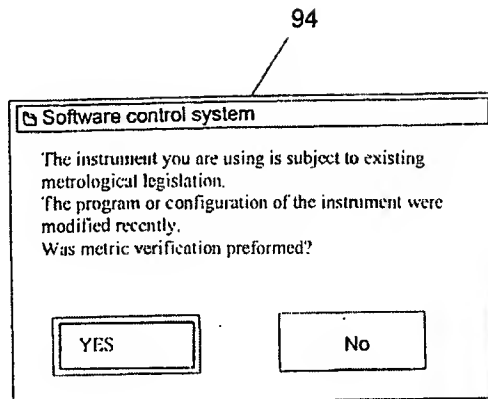
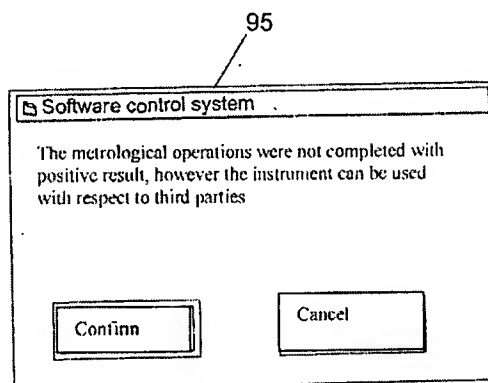
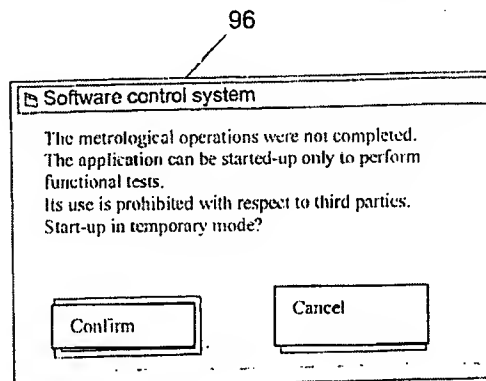


Fig. 4c



Ml 2002 A 0 0 2 4 1 9

Fig. 4dFig. 4eFig. 4f*R. E. Llanos*